

## LA-UR-21-31060

Approved for public release; distribution is unlimited.

Title: Quantum Random Number Generator (QRNG)

Author(s): Stern, Ariana Kayla

Intended for: Report

Issued: 2021-11-05

---

**Disclaimer:**

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

# Quantum Random Number Generator (QRNG)

Los Alamos National Laboratory and Qrypt, Inc.

## Innovation

The Los Alamos Quantum Random Number Generator (QRNG) is a hardware-based, high-performance Random Number Generator capable of generating 200 Mbit/s or more of true random numbers. Like flipping a coin, it is very much random and essential for information security like encrypting data on the internet, checking email, or purchasing something from an online vendor. The device harvests entropy from fluctuations in an optical source that arise from quantum mechanical properties of light. Qrypt, Inc., a company launched in 2017, began making strategic investments and developing partnerships to advance cutting-edge quantum hardware solutions. One of those key investments was licensing QRNG from Los Alamos and subsequently collaborating with advanced quantum materials and technology researcher Dr. Raymond Newell to create high-quality random keys at scale.

## Technology Advancement

The Los Alamos QRNG can meet the demands of even the highest-performance crypto-systems. This device can be used as a dedicated random number generator or deployed as the core component of an entropy-as-a-service network device. Qrypt's goal is to enable secure encryption for the modern age. Qrypt is leveraging cloud infrastructure, new algorithms, and high-rate QRNGs. The company has built the first generation of Entropy-as-a-Service using the same global infrastructure, which makes QRNGs available to any internet connected device. Qrypt distributes those random numbers via cloud services, enabling more secure cryptography for all applications and clients like banking and critical infrastructure. In order to implement this at scale, Dr. Newell is working closely with the Qrypt engineers testing and validating the circuit and optical devices.

## Impact

Qrypt licensed the Triad, LLC QRNG technology to commercialize it for its cloud-based Quantum Entropy-as-a-Service platform. Los Alamos continues to work with Qrypt under a Cooperative Research and Development Agreement (CRADA) to test and validate the QRNG technology to support its deployment into the marketplace. Together Qrypt and Los Alamos are working to make the QRNG technology a practical device that will be located inside a computer within a data center. Qrypt has started to build its first prototype and is seeing early progress and success. The goal is to begin scaling and commercializing the technology by the end of the year.



"I think it's essential that as the technologies we develop reach a certain level of technical maturity, we need to have a path forward out of the Laboratory."

- Raymond Newell,  
Los Alamos National Laboratory

## Timeline

**February, 2020:** Qrypt, Inc. Signed an agreement with Los Alamos to license specific Triad, LLC QRNG intellectual property.

**November, 2020:** Los Alamos entered into a Cooperative Research and Development Agreement with Qrypt to further develop and transition the QRNG technology to the company.